Statement before the House Homeland Security Subcommittee on Counterterrorism, Law Enforcement, and Intelligence

"Countering Threats from the CCP to the Homeland"

A Testimony by:

Kari A. Bingen

Director, Aerospace Security Project, CSIS

March 9, 2023

310 Cannon House Office Building

Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the Subcommittee, thank you for the opportunity to appear before you today to discuss "Countering Threats from the CCP to the Homeland." The Center for Strategic and International Studies (CSIS) does not take policy positions, so the views represented in this testimony are my own and not those of my employer.

I have the privilege of leading the Aerospace Security Project at the Center for Strategic and International Studies, where I examine these issues largely through a national security lens, drawing from my experiences working at a U.S. technology startup, serving in the Department of Defense (DoD) guiding defense intelligence and security activities, and supporting the House Armed Services Committee.

Conflict with China is not inevitable, but the Chinese Communist Party (CCP) has been studying the United States, studying our way of war and our vulnerabilities, expanding and modernizing its military, using its economic influence to coerce others, and putting in place the pieces to "win without fighting." As stated in the Administration's 2022 National Security Strategy, the People's Republic of China (PRC) has ambitions "to become the world's leading power" and to "reshape the international order… to its benefit."[1] For the Department of Defense, the PRC is its "pacing challenge."[2]

Beijing has undertaken a broad campaign using all tools of national power and influence – diplomatic, economic, military, technological, and informational – to achieve its aims. While strategic competition and potential military conflict with China may seem abstract to many Americans, the Chinese surveillance balloon, shot down off the East Coast on February 4, 2023, was a tangible, visible signal that the U.S. homeland is not out of reach of Beijing's threats. It is also a reminder that the CCP's broad campaign for global power status and domination in the Indo-Pacific necessitates a focus on the U.S. homeland.[3]

I offer three areas where the CCP threat to the U.S. homeland is particularly acute: technology acquisition, critical infrastructure, and influence operations.

Technology Acquisition

Beijing has made it a national goal to acquire foreign technologies to advance its economy and modernize its military. It continues to comprehensively target advanced U.S. technologies, including in areas such as high-performance computing, biopharmaceuticals, robotics, energy, and aerospace. These are among ten areas that Beijing has explicitly identified

[1] "National Security Strategy," The White House, October 12, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.
[2] "National Defense Strategy of The United States of America," Department of Defense, October 27, 2022, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf.
[3] "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February, 7, 2022, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

as high priorities in its "Made in China 2025" strategic initiative to achieve technological superiority.[4] Aerospace is an example where Chinese President Xi Jinping has articulated his "space dream" to make China the foremost space power by 2045.

To acquire these technologies, Beijing uses both licit and illicit methods to target the people, information, businesses, and research institutions in the United States that underpin them. These methods include economic espionage, cyber data exfiltration, joint ventures, research partnerships, and talent recruitment programs, among others.[5]

The Director of National Intelligence's 2018 Worldwide Threat Assessment judged that, "most detected Chinese cyber operations against U.S. private industry are focused on cleared defense contractors or IT and communications firms."[6] Over the past several years, U.S. Department of Justice convictions or indictments highlight numerous of these methods in practice. Both Chinese nationals and U.S. citizens have been charged with economic espionage and attempted acquisition of sensitive U.S. defense technology in areas such as anti-submarine warfare, aviation, and submarine quieting technology.[7] Lucrative stipends, as part of Beijing's Thousand Talents Program, were offered to researchers to bring their technical knowledge to China.[8] Chinese real estate investors sought U.S. farmland and wind farms in proximity to U.S. military bases, and Chinese telecommunications equipment (e.g., Huawei devices) has been found near U.S. missile bases, all of which could be used to surveil or disrupt U.S. defense activities.[9]

---

[4] Karen M. Sutter, "'Made in China 2025' Industrial Policies: Issues for Congress," Congressional Research Service, December 22, 2022, 1, https://crsreports.congress.gov/product/pdf/IF/IF10964/9.

[5] "Foreign Economic Espionage in Cyberspace," National Counterintelligence and Security Center, 2018, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

[6] Daniel R. Coats, "Worldwide Threats Assessment of the US Intelligence Community," Office of the Director of National Intelligence, Feb 13, 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[7] United States Attorney's Office, District of Massachusetts, "Chinese National Arrested for Conspiring to Illegally Export U.S. Origin Goods Used in Anti-Submarine Warfare to China," Department of Justice, June 21, 2018, https://www.justice.gov/usao-ma/pr/chinese-national-arrested-conspiring-illegally-export-us-origin-goods-used-anti-submarine; United States Attorney's Office, Northern District of New York, "Former GE Power Engineer Sentenced for Conspiracy to Commit Economic Espionage," Department of Justice, January 3, 2023, https://www.justice.gov/usao-ndny/pr/former-ge-power-engineer-sentenced-conspiracy-commit-economic-espionage.

[8] Ellen Barry and Gina Kolata, "China's Lavish Funds Lured U.S. Scientists. What Did It Get in Return?," The New York Times, February 6, 2020, https://www.nytimes.com/2020/02/06/us/chinas-lavish-funds-lured-us-scientists-what-did-it-get-in-return.html.

[9] Eamon Javers, "Chinese Company's Purchase of North Dakota Farmland Raises National Security Concerns in Washington," CNBC, July 1, 2022, https://www.cnbc.com/2022/07/01/chinese-purchase-of-north-dakota-farmland-raises-national-security-concerns-in-washington.html; Lars Erik Schönander and Geoffrey Cain, "China Is Buying the Farm," The Wall Street Journal, September 8, 2022, https://www.wsj.com/articles/the-chinese-are-buying-the-farm-north-dakota-hong-kong-land-food-shortage-supply-chain-usda-11662666515; Lillis, Katie Bo. "CNN Exclusive: FBI Investigation Determined Chinese-Made Huawei Equipment Could Disrupt US Nuclear Arsenal Communications." CNN, July 25, 2022. https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html.

This matters for our defense, as the PRC employs methods on American soil to funnel U.S. technology and know-how back to Beijing to advance its own military capabilities while also exploiting U.S. military vulnerabilities. The U.S. military's battlefield advantage has long rested on our superior technology. But that is at risk as Beijing seeks to close the gap in our technology advantage and become a world class military power, on par with the United States, by 2049.

This matters for American businesses. The Office of the Director of National Intelligence estimated in 2015 that the cost of economic espionage through hacking is $400 billion per year, largely attributable to the PRC. The Commission on the Theft of American Intellectual Property in 2017 estimated that the cost to the U.S. economy from stolen intellectual property (IP) could range from $225 to $600 billion annually.[10]

CCP law and policy further bolsters these methods. The CCP's military-civilian fusion (MCF) policy blurs the distinction between civil/commercial sectors and military/defense industrial sectors. It facilitates the transfer of technology and investments from the commercial sector to the military. Its national intelligence law, passed in 2017, requires that "all organizations and citizens shall support, cooperate with, and collaborate in national intelligence work… and shall protect national work secrets they are aware of."[11]

Finally, the PRC's advances in technology will undoubtedly also be fueled by its increase in research and development (R&D) expenditures and its science, technology, engineering, and math (STEM) workforce, both of which have trendlines that are increasing in China and decreasing in the United States. Data from the National Science Board shows that, over the 2000 to 2019 period, the U.S. share of global R&D declined from 37 to 27 percent while the share by China increased from 5 to 22 percent.[12] A recent study by Georgetown's Center for Security and Emerging Technology estimated that, by 2025, China's yearly STEM PhD graduates will nearly triple the number of U.S. graduates (in the same fields).[13]

The PRC challenge is one of both national and economic security. It is not only the pacing military threat for the United States, but also the top threat to U.S. technological competitiveness.

---

[10] Chris Strohm, "No Sign China Has Stopped Hacking U.S. Companies, Official Says," Bloomberg, November 18, 2015, https://www.bloomberg.com/news/articles/2015-11-18/no-sign-china-has-stopped-hacking-u-s-companies-official-says; "Update to the Report of the Commission on the Theft of American Intellectual Property," The National Bureau of Asian Research, February 2017, https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf.

[11] Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[12] Amy Burke et al., "The State of U.S. Science and Engineering 2022", National Science Board, January 18, 2022 https://ncses.nsf.gov/pubs/nsb20221/u-s-and-global-research-and-development.

[13] Remco Zwetsloot et al., "China is Fast Outpacing U.S. STEM PhD Growth," Center for Security and Emerging Technology, Georgetown University, August 2021, https://cset.georgetown.edu/publication/china-is-fast-outpacing-u-s-stem-phd-growth/.

Critical Infrastructure

The CCP is targeting critical infrastructure in the United States. I fully anticipate that – should a crisis or conflict unfold – Beijing would seek to disrupt the operations of critical infrastructure in the United States, especially early on. This could be motivated by a desire to deter U.S. action, affect U.S. decision-making, delay the mobilization of U.S. forces, or affect the will of the American people.

The DoD's annual military assessment of the PRC was stark in its assessment, "China seeks to create disruptive and destructive effects… to shape decision-making and disrupt military operations in the initial stages of a conflict by targeting and exploiting perceived weaknesses of militarily superior adversaries."[14] Both the DoD and Intelligence Community have further assessed that China could launch cyberattacks against critical infrastructure in the United States, such as oil and gas pipelines, and rail systems, that would disrupt service for days to weeks.[15]

The ransomware network hack of the Colonial Pipeline in May 2021, although not attributed to the PRC, provided a glimpse of what such disruptions could look like, with gas shortages, long lines at gas stations, and the panic buying that ensued. Similarly, the electrical grid failure in Texas in February 2021, also not the result of any PRC action, showcased the widespread impact of the loss of power for millions of Americans.[16]

The U.S. government has taken some steps to share intelligence information on PRC campaigns to target critical infrastructure. Notably, in July 2021, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released information on Chinese state-sponsored cyber intrusion campaigns, including tactics, techniques, and procedures (TTPs) that have been been employed with the aim of "holding U.S. pipeline infrastructure at risk" through physical damage to pipelines or disruption of pipeline operations.[17]

Influence Activities

The U.S. homeland is within reach of the PRC's influence activities. The PRC "conducts influence operations that target media organizations, business, academic, cultural institutions,

---

[14] "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," U.S. Department of Defense, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

[15] "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," U.S. Department of Defense, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF; "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February 2022, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

[16] "The Timeline and Events of the February 2021 Texas Electric Grid Blackouts," The University of Texas at Austin's Energy Institute, July 2021, https://energy.utexas.edu/research/ercot-blackout-2021.

[17] "Cybersecurity Advisory: Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, July 21, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a.

and policy communities of the United States."[18] As part of its "three warfares" concept, the PRC seeks to leverage psychological warfare, public opinion warfare, and legal warfare to influence decision-makers, shape public narratives, spread disinformation, and advance its interests.

Examples include TikTok, with over 100 million U.S. users that U.S. intelligence officials caution can be influenced by CCP-driven manipulation of its algorithms. They also include Operation Fox Hunt, where CCP-directed individuals spy on U.S.-based pro-democracy activists, intimidate Chinese and Chinese-American students at U.S. universities, and pressure individuals in the United States to return to China, including by threatening family members.[19] In contrast, Chinese state-run media characterize Fox Hunt as, "targeting suspected economic criminals, many of them corrupt officials."[20]

The PRC also exerts influence through its Belt and Road Initiative (BRI), including its Digital Silk Road (DSR) initiative, which involves a strategy of exporting terrestrial infrastructure, information and communications technology, and other high technology areas.[21] This global influence directly impacts U.S. businesses and U.S. security interests here at home.

One acute area of competition is in commercial satellite communications, which CSIS recently examined in a study on low Earth orbit (LEO) broadband networks.[22] These space-based constellations, such as SpaceX's Starlink and Amazon's Project Kuiper, offer a compelling solution for bridging the digital divide, specifically for rural and underserved communities, as nearly 40 percent of the world's population, and 28 percent of rural households in America remain unconnected. However, with its heavy economic presence in many BRI countries, China is positioned to negotiate concessions for its telecommunications and satellite broadband services, while discouraging the adoption of U.S. commercial services.

Further expansion of its telecommunications services could boost Beijing's presence in foreign terrestrial networks. This would provide the CCP with remote access to route data back to Beijing (as was reportedly done to the African Union Headquarters, whose network infrastructure was built and operated by Chinese entities), grant it extensive surveillance and

---

[18] "Military and Security Developments Involving the People's Republic of China: Annual Report to Congress," U.S. Department of Defense, September 4, 2020, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.pdf.

[19] Office of Public Affairs, "Eight Individuals Charged With Conspiring to Act as Illegal Agents of the People's Republic of China," Department of Justice, October 28, 2020, https://www.justice.gov/opa/pr/eight-individuals-charged-conspiring-act-illegal-agents-people-s-republic-china.

[20] Cao Yin, "Success of Fox Hunt campaign continues," China Daily, November 5, 2015, http://www.chinadaily.com.cn/china/2015-11/05/content_22375920.htm

[21] Makena Young and Akhil Thadani, "Low Orbit, High Stakes: All in on the LEO Broadband Competition," Center for Strategic and International Studies, December 14, 2022, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/221214_Young_LowOrbit_HighStakes.pdf?VersionId=vH1lp3dD7VcHGRcvuF9OdzV2WJc_KG42.

[22] Ibid.

coercive powers, enable it to block internet access or censor information, and exert greater control over international data flows.[23]

While the U.S. government has taken steps to ban Chinese telecommunications devices by Huawei, ZTE, and others, such high levels of dependence by other countries on Chinese-built and -operated digital infrastructure may lead to greater adoption of Chinese-crafted techno-authoritarian norms, standards, and data-governance practices.

Recommendations

Below are a few recommendations that I believe can help address these challenges.

- **Expand education and awareness.** This hearing is an important way to educate the American public that the threat posed by the CCP is not an abstract notion nor solely a distant military conflict that could take place across the Pacific. The American public and businesses need to understand the security and economic risks presented by the CCP and understand that they are a target of CCP influence and operations. Clearly, the U.S. homeland is not out of reach of Beijing's threats, with PRC malign activities and operations occurring here every day, below the level of armed conflict. The FBI now opens two new counterintelligence investigations nearly every day.[24] Should deterrence fail, the CCP is likely to ensure that the conflict is not contained in the Indo-Pacific but that it is felt in the United States, particularly through disruptions of critical infrastructure and influence campaigns.[25]

- **Deepen threat sharing with the private sector.** Building off CISA's work to-date, further expand threat intelligence sharing with the private sector. Encourage the downgrading of intelligence and provide security read-ons for business leaders across critical infrastructure sectors, e.g., energy, water, and financial services. Examples like the 2021 CISA advisory on oil and gas pipeline cyber threats, where specific TTPs attributable to Chinese state actors were shared, enable companies to better understand their vulnerabilities, the sophistication of adversary threats, and to make risk-informed decisions regarding protection and resiliency measures.

- **Transform counterintelligence (CI) and security missions.** CI and security missions have traditionally involved manual, labor-intensive processes, from espionage casework to background investigations for security clearances to defense industry site visits for inspections. The scale of the CCP threat, the various methods it uses for acquiring

[23] Abdi Latif Dahir, "China 'Gifted' the African Union a Headquarters Building and Then Allegedly Bugged It for State Secrets," Quartz, January 30, 2018, https://qz.com/africa/1192493/china-spied-on-african-unionheadquarters-for-five-years.
[24] Remarks by FBI Director Christopher Wray at the Ronald Reagan Presidential Library and Museum, January 31, 2022, Simi Valley, CA, https://www.fbi.gov/news/stories/director-wray-addresses-threats-posed-to-the-us-by-china-020122.
[25] "Military and Security Developments Involving the People's Republic of China: Annual Report to Congress," U.S. Department of Defense, September 4, 2020, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.pdf.

technology, and the sheer volume of data that could be tapped into, necessitate adapting the tradecraft for these challenges. This includes incorporating new technologies, approaches to, and additional resources for the mission. For example, how can big data and artificial intelligence/machine learning (AI/ML) help identify supply chain vulnerabilities, monitor abnormal cyber activities, track foreign agents, and illuminate disinformation? How can CI analysts work with technology startups, on relevant business timelines, to prevent investment deals that involve adversarial capital?

- **Leverage technology innovation.** Maintaining U.S. technological leadership means not just preventing the transfer of technology to the PRC, but also setting the conditions for our innovation sector to prosper and to stay ahead of the competition. We are in a period of rapid technological change, with the commercial sector leading in many areas of technological innovation. The government should seek greater adoption and integration of commercial technologies to support mission needs, taking advantage of their speed, agility, and the private capital being invested in them.

- **Boost cooperation with allies and partners.** Our alliances and partnerships are a competitive advantage and source of strength that the CCP does not have. In order to lessen this advantage, China is actively trying to divide and weaken U.S. alliances and partnerships.[26] Our technology is soft power for the United States, and technology cooperation can be a strong feature of these relationships while also bolstering our private sector innovation base. But increasing cooperation will require revisiting U.S. technology control policies. We need to strike the right balance between protecting our sensitive technology, recognizing Beijing's extensive efforts to steal it, and enabling American companies to be the partner of choice for our allies and partners.

- **Continue investing in a strong defense.** Continued investment in a strong defense is required to deter PRC aggression, build resiliency to attack, and ensure we have the trained people, posture, intelligence, weapon systems, and munitions to defend the United States and the American people.[15]

Thank you again for your time today and I look forward to your questions.

# #

[26] Seth G. Jones, "Empty Bins in a Wartime Environment: The Challenge to the U.S. Defense Industrial Base," Center for Strategic and International Studies, January 23, 2023, https://www.csis.org/analysis/empty-bins-wartime-environment-challenge-us-defense-industrial-base.

Statement before
the Subcommittee on Counterterrorism,
Law Enforcement, and Intelligence
U.S. House of Representatives (118th Congress)

Hearing on
"Confronting Threats Posed by the
Chinese Communist Party to the U.S. Homeland"

A Testimony By

Tyler Jost, Ph.D.
Watson Institute Assistant Professor of China Studies
Assistant Professor of Political Science, International & Public Affairs
Department of Political Science
Brown University

March 9, 2023

Chairman Pfluger, Ranking Member Magaziner, and distinguished members of the Committee, thank you for the opportunity to testify before the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence. My remarks today will focus on two areas: (1) the broader strategic context through which China's overseas intelligence collection and information campaigns should be viewed; and (2) what the currently available evidence can tell us about the scope and effectiveness of these campaigns.

My testimony today is given as a scholar of Chinese foreign policy and U.S.-China relations. I emphasize this for two reasons. First, my role in academia is one of a researcher, rather than an administrator. My testimony is not on behalf of or directly or indirectly associated with my employer. Second, as former intelligence officer in the U.S. military, I am well aware that some of the most detailed reporting on a topic as sensitive as homeland security remains classified. As such, the testimony I am best positioned to offer pertains to the scholarly conclusions that can be drawn based on publicly available research.

To summarize, my assessment regarding China's threat to the U.S. homeland is threefold. First, it is clear that China is interested in using its capabilities to gather information and promote narratives that are consistent with its interests. Second, publicly available research provides inconclusive evidence regarding the effectiveness of China's operations, particularly those aimed at shaping global public opinion. Third, the U.S. government should consider devoting more resources toward research that can more precisely and conclusively assess the level of threat posed by China's activities in the United States. The absence of authoritative and publicly available evidence does not necessarily confirm the ineffectiveness of China's actions, but leaves observers without a clear picture of how to rank the severity of these threats in comparison to other aspects of American foreign policy toward China, such as the emerging bilateral security competition and the possibility of future military conflict.

The Context of U.S.-China Strategic Competition

The competition between the United States and China represents one of the defining international challenges of this century. In my view, the central problem of the U.S.-China relationship continues to be how to manage the two issues that most divide Washington and Beijing.

The first is that the United States and China have potentially irreconcilable differences over Taiwan. These differences have been effectively managed for decades, but both sides are increasingly apprehensive about the ability to maintain the status quo. There is healthy debate among scholars as to what is driving recent apprehensions. Some emphasize changes to the balance of power.[1] Others emphasize the difficulties of credible assurance, which might cause Beijing to feel it has no choice but to take military action.[2]

These dynamics are primed to put the United States in a difficult position. If the United States hopes to deter future military action against Taiwan, it will need to do one of the following: (1) match Chinese capabilities in the region to keep the costs of conflict prohibitively high; (2) reassure Beijing that the United States and Taiwan will not change the status quo, assuming that such concerns are central to Beijing's decision-making; or (3) some combination of the two. If the United States does not manage this aspect of the bilateral relationship effectively, deterrence may fail. The consequences of such a conflict would be devastating, not only in terms of the human and economic costs imparted on both sides, but also in terms of the reputational toll to the credibility of American strategic judgement if it fails to win. The stakes of successfully navigating this issue could not be higher.

The second issue is that the United States and China eye each other's domestic institutions with suspicion. Chinese decision-makers think about national security as the security of the regime.[3] From the perspective of Beijing's leaders, one of the most formative events in the country's history was the collapse of communist regimes in Eastern Europe, followed by the Soviet Union, which demonstrated the possibility of a similar fate for the Chinese Communist Party.[4] Beijing views some, although not all, of the global rules and norms that emerged after the Cold War as threats to the regime's stability, particularly those regarding the effectiveness and appropriateness of democratic institutions.[5]

Thus, while it is important to seriously evaluate the threats that China poses to the homeland, these inquiries should not distract attention from the issues that are likely to be central in the global competition – and will greatly shape whether the two sides end up in what could be the most costly and dangerous conflict between two major powers since 1945.

---

[1] Heginbotham, Eric, et al. *The US-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017*. Santa Monica: Rand Corporation, 2015; Kastner, Scott L. "Is the Taiwan Strait Still a Flash Point? Rethinking the prospects for armed conflict between China and Taiwan." *International Security* 40.3 (2015): 54-92.

[2] Blanchette, Jude and Ryan Hass. "The Taiwan Long Game: Why the Best Solution Is No Solution." *Foreign Affairs*. 102.1 (2023): 102-114; Weiss, Jessica Chen. "The U.S. Should Deter – Not Provoke – Beijing over Taiwan." *The Washington Post*. February 20, 2023.

[3] Weiss, Jessica Chen. "A World Safe for Autocracy?" *Foreign Affairs* 98.4 (2019): 92-108; Greitens, Sheena Chestnut. "Internal Security & Grand Strategy: China's Approach to National Security Under Xi Jinping." *Statement before the US-China Economic and Security Review Commission, Hearing on US-China Relations at the Chinese Communist Party's Centennial* (2021).

[4] Sarotte, Mary Elise. "China's Fear of Contagion: Tiananmen Square and the Power of the European Example." *International Security* 37.2 (2012): 156-182; Gewirtz, Julian. *Never Turn Back: China and the Forbidden History of the 1980s*. Cambridge: Harvard University Press, 2022.

[5] Johnston, Alastair Iain. "China in a World of Orders: Rethinking Compliance and Challenge in Beijing's International Relations." *International Security* 44.2 (2019): 9-60.

CCP Activities Abroad

It is helpful to view China's activities toward the U.S. homeland in this context. Like many countries, China seeks to gain advantages over states with whom it has differences in order to improve its bargaining power. The more intelligence that China is able to collect regarding foreign military capabilities, for instance, the more they might be able to emulate those capabilities within their own military portfolio, with an eye toward bargaining hard for the two priority issues discussed above.

China's overseas activities that emerge from this strategic context can be loosely divided into two categories. The first focuses on intelligence collection. The second focuses on information distribution. It is important to distinguish these two areas, because each is quite different in terms of the nature, scope, and potential to impart costs on the United States.

Intelligence Collection

In terms of intelligence collection, it is well-documented that China is gathering data in order to improve its military capacity, provide insight into U.S. decision-making processes, and potentially gain a tactical advantage over the United States in the event of a future conflict. The recent incident in which a Chinese high-altitude balloon traversed American airspace illustrates in vivid fashion that China is willing to assume risks in order to gather data against U.S. targets.

The fact that this event occurred shortly before Secretary of State Anthony Blinken's planned diplomatic visit to China is noteworthy. If recent reporting from the U.S. Department of Defense stating that Xi Jinping was unaware of the timing of this particular mission is true, it suggests that Beijing may have delegated decision-making regarding tactical execution of these operations to bureaucratic stakeholders who had limited understanding of how the disclosure of such an intelligence mission could shape China's other strategic priorities.[6] Such a posture could imply that Beijing has a high level of risk tolerance in its intelligence collection.

There are equally concerning aspects the security of personal data. Investigations into Chinese intelligence have long noted Beijing's interest in collecting data on foreign citizens, demonstrated by the 2015 Office of Personnel Management data breach and the 2017 cyber espionage operation against Equifax.[7] These events, coupled with the technical realities of digital technologies, illustrate that government communications and the privacy of American citizens may both potentially be compromised through the use of foreign hardware and software.

It seems more than plausible that China's defense espionage campaign has contributed to its ability to develop more advanced military technologies, which could shape its ability to fight and win a war in the Asia-Pacific region.[8] There is less publicly available reporting to document whether these intelligence operations, which have been successful at the collection phase, have also been effective in advancing Beijing's broader diplomatic, economic, and security goals beyond defense production.

---

[6] Eric Schmitt and Zach Montague. "Balloon Crisis Highlighted a Split in China's Leadership, Pentagon Official Says," *The New York Times*, February 17, 2023.

[7] David E. Sanger and Julie Hirschfeld Davis. "Hacking Linked to China Exposes Millions of U.S. Workers," *The New York Times*, June 4, 2015; Katie Benner. "U.S. Charges Chinese Military Officers in 2017 Equifax Hacking," *The New York Times*, May 7, 2020.

[8] Department of Defense. *Report on Military and Security Developments Involving the People's Republic of China*, 2022, 147, 153.

Simply collecting data, particularly in large quantities, is insufficient to help decision-makers achieve their goals.[9] I am unaware of any publicly available study that has been able to document such a connection in the recent past. Recognizing this gap in our understanding is important, not only because it should drive the United States' own intelligence collection priorities, but also because we should recognize the challenges Beijing will face in effectively managing such large amounts of data.

Shaping Global Public Opinion

In parallel to intelligence collection, China engages in operations to disseminate information to foreign audiences. To date, the bulk of these activities are aimed at shaping global public opinion.[10] In simplest terms, China presents foreign citizens with information with the hope that it will shape the target's attitudes and, possibly, behavior. Perhaps the most concerning facet of these activities occurred last fall, when Meta and Google each reported that China-based groups had disseminated political content prior to the 2022 midterm elections.[11]

The idea of information control and propaganda is deeply embedded in the Chinese Communist Party's institutions – and it is easy to see how this would naturally spill over into efforts to shape public opinion abroad.[12] They also tie into the second core issue motivating the bilateral competition: China's concern about regime survival and the threat that a lack of international status might have on the Party's continued ability to rule. Furthermore, it is plausible that China genuinely believes that the rest of the world misunderstands it – and that these misunderstandings can be rectified through methods similar to those it employs at home.

These efforts to shape foreign public opinion through party propaganda are real and their scope broad. It is estimated that China spends approximately $8 billion on public diplomacy efforts alone.[13] To date, however, there is limited publicly available research documenting whether China's operations to shape foreign attitudes have been effective. For example, China Global Television Network (CGTN), a broadcasting company affiliated with the Chinese state, is actively disseminating China's public messaging worldwide.[14] But there are few studies that apply validated research methods for estimating the causal effect of exposure to such messages on public opinion.

The available evidence suggests several reasons why these operations might actually prove to be less effective than we might fear. Broadly, efforts to shape foreign public opinion do not always work out the way that states hope. Some research suggests, for example, that salient components of China's public diplomacy initiatives do not improve foreign attitudes toward China.[15] Scholars at Yale

---

[9] Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford: Stanford University Press, 1962.
[10] Diamond, Larry, and Orville Schell, eds. *Chinese Influence and American Interests: Promoting Constructive Vigilance*. Stanford: Hoover Institution Press, 2018; Brazys, Samuel, and Alexander Dukalskis. "China's Message Machine." *Journal of Democracy* 31.4 (2020): 59-73.
[11] Kurlantzick, Joshua. "China's Growing Attempts to Influence U.S. Politics." *Council on Foreign Relations*, October 31, 2022.
[12] King, Gary, Jennifer Pan, and Margaret E. Roberts. "How Censorship in China Allows Government Criticism But Silences Collective Expression." *American Political Science Review* 107.2 (2013): 326-343; Roberts, Margaret E. *Censored: Distraction and Diversion Inside China's Great Firewall*. Princeton: Princeton University Press, 2018.
[13] Martin, Peter. *China's Civilian Army: The Making of Wolf Warrior Diplomacy*. New York: Oxford University Press, 2021, 213.
[14] Diamond and Schell 2018, 103.
[15] Green-Riley, Naima. *How States Win Friends and Influence People Overseas: The Micro-Foundations of U.S. and Chinese Public Diplomacy* (PhD Thesis). Harvard Department of Government.

University have found that Twitter messaging by Chinese diplomats were only able to positively shape perceptions of China when the message was framed in positive terms. When Chinese diplomats instead resorted to nationalist messages, often termed "Wolf Warrior" diplomacy, Twitter messages instead had a negative effect on foreign public opinion.[16]

Some of the best available evidence on the domestic effects of China's propaganda also suggests that such messages do not necessarily operate as one might think. Several experimental studies have found that propaganda inside China can backfire, causing Chinese citizens to adopt less favorable views toward the government.[17] It is worth noting, however, that these studies have also found that Chinese propaganda is effective in signaling the strength of the state. That is, propaganda does not always change political attitudes, but it does remind citizens of the CCP's ability to coerce. Other studies suggest that Chinese domestic propaganda can be effective when it is able to emotionally resonate with its citizens, such as through nationalistic narratives recounting past wars in a positive light.[18] However, it is not yet clear that these same methods can be effectively applied in foreign countries.

One possible reason that Chinese propaganda could fail to sway global public opinion as intended is that foreign audiences may ascribe malign intentions to foreign governments, especially China. Research suggests that the ability to sway political attitudes depends in part on whether a target audience believes that what social scientists term the "cue-giver" (in this case China) has the audience's best interests at heart.[19] To illustrate this point in more familiar terms, consider how an American voter may be more likely to update their political attitudes when they receive a message from a co-partisan than when they receive one from a member of another party. There is an intuitive logic behind this: people make general judgments about who they deem trustworthy (e.g., one who shares the same basic political values) and then prioritize messages from these sources as they wade through the vast amounts of information to which they are exposed in daily life.[20]

Applying this intuition to China's public messaging campaigns would suggest that American citizens may be predisposed to severely discount or even completely discard messages received from Chinese propaganda outlets, provided that their baseline trust of such sources is low and they are able to accurately identify the creator of the content. Some studies of public diplomacy in other country contexts, usually focusing on the ability of American officials to shape global public opinion, are congruent with this conclusion.[21] Other experimental studies find a similar effect with regard to American perceptions of foreign public diplomacy as well.[22]

---

[16] Mattingly, Daniel C., and James Sundquist. "When Does Public Diplomacy Work? Evidence from China's 'Wolf Warrior' Diplomats." *Political Science Research and Methods* (2022).
[17] Huang, Haifeng. "Propaganda as Signaling." *Comparative Politics* 47.4 (2015); Huang, Haifeng. "The Pathology of Hard Propaganda." *The Journal of Politics* 80.3 (2018): 1034-1038.
[18] Mattingly, Daniel C., and Elaine Yao. "How Soft Propaganda Persuades." *Comparative Political Studies* 55.9 (2022): 1569-1594.
[19] Lupia, Arthur, Mathew D. McCubbins, and Lupia Arthur. *The Democratic Dilemma: Can Citizens Learn What They Need to Know?* New York: Cambridge University Press, 1998.
[20] Druckman, James N. "On the Limits of Framing Effects: Who Can Frame?" *The Journal of Politics* 63.4 (2001): 1041-1066.
[21] Goldsmith, Benjamin E., and Yusaku Horiuchi. "Spinning the Globe? US Public Diplomacy and Foreign Public Opinion." *The Journal of Politics* 71.3 (2009): 863-875.
[22] Rhee, Kasey, Charles Crabtree, and Yusaku Horiuchi. "Perceived Motives of Public Diplomacy Influence Foreign Public Opinion." *Political Behavior* (2023).

In addition, trends in global public opinion should provide some comfort. If one judges the effectiveness of China's public diplomacy campaign based solely on China's approval rating in foreign countries, the effort has been a catastrophic failure. This is true not only in the United States, but in Japan, Australia, South Korea, and much of Europe as well. Across these countries, China is less well-trusted today that it was ten years ago. China may be attempting to win hearts and minds globally, but they have not succeeded in many contexts.[23]

If China's public diplomacy campaign has backfired (i.e., the effect of the program has been in the opposite direction than Beijing intended), it would be unsurprising not only for the reasons cited above, but also because China has often miscalculated in its foreign policy decision-making. For example, one scholar at the University of Southern California has shown that China's attempts to use economic statecraft to advance its relationships with other countries are often ineffective, particularly when the target state is a democracy.[24] Several of China's international security crises, ranging from the 1969 Sino-Soviet Border Conflict to the 1979 Sino-Vietnamese War, failed to achieve many of the strategic objectives toward which Beijing's use of force was aimed.[25] In short, Beijing's ability to get what it wants in world politics is far from unchecked.

Three points of caution are merited with regard to these data. First, the aggregate relationship between a more active public diplomacy campaign and less favorable public opinion toward China is confounded by other events, particularly the COVID-19 pandemic. This implies that China could be able to shape public opinion abroad more effectively as the pandemic ends. Second, while the decline in public opinion toward China is well-documented in developed countries, these polls often do not include countries from the Global South, which may be a priority for Chinese decision-makers. Third, none of the research discussed above addresses the possibility that China could use fake online profiles to hide the source of China's messaging from foreign audiences.

Policy Recommendations

By emphasizing gaps in public knowledge, I am not suggesting that we can dismiss the potential threats that China poses to the U.S. homeland. The fact that China has demonstrated its intent to engage in both intelligence collection and efforts to shape foreign public opinion, coupled with the competitive nature of the bilateral relationship, is sufficient cause for serious attention. Rather, my hope is that emphasizing what we do and do not yet know can illuminate recommendations for policy.

1. *Fund Social Science Research on the Topic*. The U.S. government should devote resources toward publicly accessible research that fills gaps in our knowledge regarding China's activities abroad. The social sciences are in the early stages of understanding whether and how new types of social media, sometimes employed by foreign actors, can shape public opinion. It is worth emphasizing again that existing research is insufficient to determine how costly these new technologies will be to the U.S. homeland. Yet, U.S. policymakers should be open to the possibility that better research on the topic would, for example, lead to the conclusion that

[23] Silver, Laura, Christine Huang and Laura Clancy. "How Global Public Opinion of China Has Shifted in the Xi Era." *Pew Research Center*, September 28, 2022.
[24] Wong, Audrye. "How Not to Win Allies and Influence Geopolitics: China's Self-Defeating Economic Statecraft," *Foreign Affairs*. 100.3 (2021), 44-53.
[25] Jost, Tyler. "Authoritarian Advisers: Institutional Origins of Miscalculation in China's International Security Crises," *International Security*, forthcoming.

China's capacity to shape American public opinion is low – and the broader conclusion that U.S efforts might be better directed toward other parts of the competitive relationship.

2. *Protect U.S. Researchers in China.* The U.S. government should work to ensure that American scholars who choose to conduct field research in China are protected.[26] Our ability to answer many of the most pressing questions regarding the future of the competition between the United States and China is increasingly limited by restrictions on American scholars by the Chinese government. The U.S. government should use diplomatic channels to reestablish opportunities for American researchers to study the Chinese political system while feeling protected from potential exploitation and detainment by Chinese authorities.

3. *Build Evidence-Based Public Awareness.* The U.S. government needs to explain the threats that China poses the privacy of their data to the American public. Specifically, it needs to provide more detailed explanations of the different risks that American citizens assume when they use foreign and domestic technologies. This may seem obvious to individuals who have served in government, but the social appeal of these technologies will raise the burden of proof for U.S. policymakers to convince American citizens.

[26] For an overview, see Greitens, Sheena Chestnut, and Rory Truex. "Repressive Experiences Among China Scholars: New Evidence from Survey Data." *The China Quarterly* 242 (2020): 349-375.

Mitchell Institute for
Aerospace Studies
1501 Langston Boulevard
Arlington, VA 22209
http://www.mitchellaerospacepower.org

Statement for the Record
House Armed Services Committee
Lt Gen Joseph T. Guastella,
Mitchell Institute for Aerospace Studies
March 9, 2023

Chairman Pfluger, Ranking Member Magaziner, Members of the Committee, thank you for the opportunity to appear before you today. As an individual who spent over three decades in service to our nation, I am deeply concerned about the threats the Chinese Communist Party (CCP) poses to the U.S. homeland. That is why events like today's hearing are so important.

In my last assignment on Active Duty, I served as the Deputy Chief of Staff for Operations at Headquarters U.S. Air Force, where I was charged with leading the development and implementation of policy directly supporting global operations, force management, weather, training and readiness across air, space and cyber fields. To this end, I am well versed in the threat China poses to the United Sates and the capabilities they have to manifest their objectives. It was my job to oversee airpower capabilities and capacity so that our combatant commands could respond to these challenges every day—and this included the homeland defense mission of North American Aerospace Defense Command (NORAD) / Northern Command (NORTHCOM).

I would first like to begin by describing the threat China poses to the United States and its allies. In the 1991, when the U.S. was celebrating the end of the Cold War and victory in Operation Desert Storm, China made a concerted decision to modernize their military capabilities as a key ingredient in empowering their ascent as a leading military superpower.

Three decades later, they have largely met this mark and they seek further progress—that is why this year saw a marked increase in their defense spending. Their military now enjoys leading-edge capabilities that include long-range precision strike, hypersonic medium-range ballistic

missiles, sophisticated integrated air defense system (IADS) comprised of stealthy fighter aircraft like the J-20 aircraft, surface-to-air missiles (SAMS), and electronic warfare (EW) units. These capabilities radically complicate the operating environment for U.S. forces and could portend significant combat attrition, especially for forward operating bases and the non-stealth portions of America's combat air arm which makes up a vast portion of Air Force aircraft. Several of these offensive systems have the range to hold U.S. territory at risk, affecting us right here in the homeland.

The Chinese spy balloon, which garnered significant attention this past February, should serve as a wakeup call regarding the CCP's global ambitions. China's space-based intelligence, surveillance, and reconnaissance capabilities also gather information regarding the U.S. homeland. Nor are all these long-range systems passive threats. China's quest to field a 'fractional orbital bombardment system'—a long range missile that transits space enroute to its target—are not capabilities designed to secure China's immediate borders. They are part of a strategic global strike system. The U.S. must take note.

Unfortunately, the U.S. is stretched thin when it comes to the capabilities and capacity required to defend our homeland. NORAD was originally designed to detect and defend North America from a catastrophic attack from the Soviet Union, later Russia. An additional role was added after 9/11: to intercept, identify, and redirect unidentified aircraft heading toward restricted airspace. So, the NORAD radars were optimized and tuned to detect aircraft that meet those criteria.

Balloons—until recently—generally do not fit into that category. As the threat evolves, including balloons, stealth aircraft, UASs and cruise missiles…. so must our detection and defense enterprise. This will require that we modernize current radars and install new radars to cover emerging zones of vulnerability, not just over our nation but well outside our sovereign territory. Approaches to our homeland China would use are far different than those used by Russia. We must invest new resources in the NORAD mission. The command gets its aircraft from the Air Force, but our Air Force today is the oldest and smallest it's ever been in its history.

The balloon intrusions should be a wakeup call to rebuild our air and space defenses—we are still flying B-52s over 60 years old; tankers over 50; and fighters over 30. Homeland defense doesn't start in the homeland. It starts abroad with the combatant commands having credible offensive punch to hold targets at risk in adversary countries. The Air Force needs to be modernized in the numbers necessary to meet the demands of our national defense strategy, and to deter threats against our homeland.

More specifically, consider that the Air Force's fighter inventory is too small to meet real-world demand. This is a major security concern, for while other service branches possess fighter aircraft, the Air Force is specifically tasked with the homeland security air sovereignty mission.

In 1991, the Air Force possessed 4,459 fighters. Today, it has 2,221. This represents a 49 percent reduction in capacity—the majority of which were produced in the Cold War. However, this decrease in volume is not matched with a drop in operational demand. Quite the contrary given that the Air Force has been meeting non-stop combat requirements since Desert Storm in 1991. As the numbers of fighters decreased, the workload assigned to the remaining aircraft increased. They are now physically worn out and must be retired. Fourteen years ago, a Congressional Budget Office report concluded: "By 2009, 80 percent of the [Air Force's fighter] aircraft had used more than 50 percent of their originally planned service life. Clearly, the Air Force's fighter fleet is wearing out."[1] Circumstances have not improved over the ensuring decade, in fact, they have gotten worse. That is why you saw F-15C/Ds fighter aircraft withdrawn from Kadena Air Base in the Pacific this past year—not because the Air Force wanted to do this, but because the aircraft were so old they had to be retired and there were not enough new fighters to backfill them. Think of the signal that sent to China.

The simple reality is that Air Force has lacked funding necessary to procure a sufficient volume of new fighters to ensure the outflow of aging aircraft is matched by the inflow of newer examples. They have ranked third—behind the Army and Navy—in terms of Department of

[1] Congressional Budget Office (CBO), *Alternatives for Modernizing U.S. Fighter Forces* (Washington, DC: CBO, May 2009), p. 55

Defense funding for the past three decades.[2] That manifested very real results. Consider that the Air Force's leading 5th generation fighter, the F-22, had its production terminated at less than twenty five percent of the original requirement. In the 2000s, leaders outside the Air Force thought the era of peer conflict was over. They were wrong. Nor is this a one-off example, with the production ramp rate of the F-35 lagging dangerously behind original intentions. In 2020, the Air Force was supposed to have 800 F-35As in its inventory, but instead only had 272.[3]

The Air National Guard, the entity which bears the preponderance of the homeland defense mission is particularly hard hit by gap between older aircraft aging out and a lack of new aircraft arriving to backfill their spots on the ramp. The Air National Guard tends to fly older fighters, so they are a fleet lead indicator for the broader Air Force. What happened at Kadena will be replicated throughout bases across America absent rapid intervention to reset the Air Force's fighter force.

Homeland defense also requires investment and modernization in command and control, resiliency, ground and space-based sensors, data fusion technology, AI, and air refueling capabilities. Homeland defense is our highest priority mission, we need to start treating it that way.

We also lack sufficient capabilities and capacity to defend against a concerted air and missile attack at our forward bases. On January 8, 2020, eleven Iranian ballistic missiles struck U.S. forces based at the Ayn al Asad military complex in Iraq. I was the Coalition Forces Air Component Commander at the time. Our leadership possessed intelligence signaling the attack would happen, we were able to detect the missiles being launched, and we could track their trajectory. However, when it came to defeating these missiles, we lacked viable options because the joint force lacked sufficient missile defense *capacity* given other global commitments. American service members and many allies had to ride out the attack and hope for the best. That

[2] David Deptula and Mark Gunzinger, *Decades of Air Force Underfunding Threaten America's Ability to Win* (Arlington, VA: Mitchell Institute for Aerospace Studies, 2022), p. 3
[3] John A. Tirpak, "Keeping 4th-Gen Fighters in the Game," Air Force Magazine, October 1, 2019.

was an appalling set of circumstances. Think if that had happened in your hometown or key bases here in America.

Adversaries like China understand these vulnerabilities. The United States is gradually waking up to this reality, but leaders have yet to seriously address the shortfall. Note how difficult it is to provide effective, sustainable solutions to Ukraine—guarding against everything from air strikes, drone attacks, and missile bombardment. We are still in a "problem admiring" phase, not in a "solution implementation" window. This must change.

It is worth remembering that some of the first responders on the morning of 9/11 were airmen. Two off them quickly scrambled from Andrews Air Force Base to intercept a hijacked airliner bound for the nation's capital. We had no time to arm those F-16s because in the post-Cold War era, we *thought* our homeland was safe—we had stopped sitting alert. That meant those airmen were prepared to sacrifice their lives to bring down that hijacked aircraft. The passengers on Flight 93 bravely took matters into their own hands before our airmen were asked to make that sacrifice. The point in telling this story is to highlight that we have the bravest men and women in uniform. But we owe it to them to ensure they are prepared for the mission we ask them to execute. We also owe it to our citizens, to ensure they are protected from attack. America's homeland is no longer a sanctuary. We must recognize this new reality and aggressively close critical gaps in capacity and capabilities for homeland defense. Thank you for focusing on this topic today. With that, I look forward to your question.

STATEMENT OF WILLIAM R. EVANINA
CEO, THE EVANINA GROUP

BEFORE THE HOUSE HOMELAND SECURITY SUBCOMMITTEE ON COUNTERTERORISM, LAW ENFORCEMENT AND INTELLIGENCE

AT A HEARING REGARDING "CONFRONTING THREATS POSED BY THE CHINESE COMMUNIST PARTY TO THE U.S. HOMELAND.

MARCH 9, 2023

Chairman Plfuger, Ranking Member Magaziner, and Members of the Subcommittee — it's an honor to appear before you today. I have spent 32 years of my adulthood working the U.S. Government. Twenty-four of which with the FBI, CIA, and NCSC.

I was tremendously honored to be the first Senate Confirmed Director of the National Counterintelligence and Security Center (NCSC) in May of 2020.

I am here before you today as the CEO of The Evanina Group, LLC. In this role, I work closely with CEOs, Boards of Directors, and academic institutions to provide a strategic approach to mitigating risk in a complicated global environment.

THE CHINA THREAT

Our nation faces a diverse, complex, and unprecedented sophisticated threats by nation state actors, cyber criminals, and terrorist organizations.

However, the existential threat our nation is from the Communist Party of China (CCP). This threat is the most complex, pernicious, strategic, and aggressive our nation has ever faced. It is an existential threat.

We must first clearly understand this threat. We must also continue to mitigate this threat with a whole-of-society approach. We must also approach this comprehensive and holistic threat with the same sense of urgency, spending, and strategy…. As we have done for the past two decades in preventing terrorism.

I would offer to this subcommittee that we ARE in a terrorism event. A slow, methodical, strategic, persistent, and enduring event which requires a degree of urgency of action. It is clear that under Xi Jinping, the CCP's economic war with the U.S. is manifested itself into a terrorism framework.

Let me be more specific. The CCP's capabilities and intent are second to none as an adversary. They cyber breaches, insider threats, surveillance and penetrations into our critical infrastructure have all been widely reported and we have become numb to these episodes, as a nation. Add in the CCP's crippling stranglehold so many aspects of our supply chain and what results is an imbalance and vulnerability of unacceptable proportions. When we move to new areas of the CCP to include surveillance balloons, ZPMC cranes at out maritime ports, Huawei, and TikTok, the collage begins to paint a bleak mosaic.

I would ask the subcommittee is it not terrorism when a hospital, high school, police department, college, county services, or water treatment facility are shut down by a cyber breach or ransomware event? How about a natural gas pipeline that is shut off via a malware or virus? How about our electrical grid or natural gas being shut off in the winter in the Northeast part of the U.S. resulting in millions of households, and buildings, without heat? How about our telecommunications infrastructure going down one day because Verizon and AT&T are hit with a cyber-attack on the same day? Or, our financial services sector having to go offline, for even a few hours, would cause significant international chaos and disruption. Are these not terror events? "Terror" must be redefined beyond our framework which includes loved ones dying from a kinetic event.

It is easy to parlay all the "would be" and "could be" scenarios as fear-based paranoia. However, intelligence and law enforcement professionals, cyber professionals and international organizations have all seen the intent, capabilities deployed by the CCP. The inability or unwillingness to look behind the curtain and visualize this existential threat is no longer an option for anyone. There is no more curtain to look behind.

WHERE IS THE THREAT?

The U.S private sector, academia, research and development entities, and our core fabric of ideation has become the geopolitical battlespace for China.

Xi Jinping has one goal. To be the geopolitical, military, and economic leader in the world. XI, along with the China's Ministry of State Security, People's Liberation Army, and the United Front Work Department, drive a

comprehensive and whole of country approach to their efforts to invest, leverage, infiltrate, influence and steal from every corner of U.S. success.

Economic security is national security. Our economic global supremacy, stability, and long-term vitality is not only at risk, but squarely in the cross hairs of Xi Jinping and the communist regime. This is a generational battle for XI and the CCP, it drives their every decision, particularly geopolitically. How to counter and push past the U.S. is goal number one for XI and the CCP.

HOW DOES THE THREAT MANIFEST?

Intelligence services, science & technology investments, academic collaboration, research partnerships, joint ventures, front companies, mergers and acquisitions, and outright theft via insiders and cyber intrusions, begin the comprehensive and strategic framework for how China implements their strategy.

China continues to utilize "non-traditional" collectors to conduct a plurality of their nefarious efforts here in the U.S. due to their successful ability to hide in plain sight. The non-traditional collectors, serving as engineers, businesspersons, academics, and students are shrouded in legitimate work and research, and oftentimes become unwitting tools for the CCP and its intelligence apparatus.

China's ability to holistically obtain our Intellectual Property and Trade Secrets via illegal, legal, and sophisticated hybrid methods is like nothing we have ever witnessed. Joint ventures, creative investments into our federal, state and local pension programs, collaborative academic engagements, Sister City Programs, Confucius Institutes on Campus, Talent Recruitment Programs, investments in emerging technologies, and utilization of front companies continue to be the framework for strategically acquiring the thoughts and ideas of our researchers, as well as development of those ideas pre and post patent application. The threat from China pertaining to academia is both wide, and deep. The past six years of indictments and prosecutions have highlighted the insidiousness of China's approach to obtaining early and advanced research as well as understanding the complexity of gifts and funding at U.S. colleges and universities, particularly when tied to federal grants.

INDUSTRIES LEADING AS TARGETS

China's priorities for obtaining U.S. based technology and know-how, pursuant to their publicly available "Made in China 25 Plan" are Aerospace, Deep Sea Technology, Biotechnology, Information Technology, Manufacturing, Clean Energy, Electric Battery Technology, and DNA/Genomics.

Any CEO or Board of Directors leading in any of these critical industries must become aware of the threat posed to them and work with their security team and outside experts to identify risk-based mitigation strategies.

LONG TERM CONSEQUENCES OF IP THEFT

The proverbial salt in the wound of the China's nefarious activity is when the CCP steals our thoughts, ideas, patents, and technology, and manufactures that same technology in China, and the sells it back to American companies and around the world. One needs to look no further than the American Supercomputer Corporation for just a glimpse of the long-term impact to economic espionage.

Then one must factor in all the manufacturing plants which were are not built, and the tens of thousands of jobs which were not created because China, via its theft, beat the U.S. to the global market and is selling the same product and a significant reduction in real costs.

Currently prescient is the passage of the CHIPS and Science Act, as well as the Inflation Reduction Act. Rest assured, China has already begun their strategic, and comprehensive, efforts to acquire (both legally and illegally) any and all ideation, research, and trade secrets emanating from the extensive funding provisions and technological incentives, provided by these legislative actions.

I would offer emerging renewable energy technologies, and semiconductor production will be targeted most aggressively. Congress must lead and hold everyone accountable for assuring that ten years from now Congress cannot be holding hearings and asking how China stole our technology, and capabilities, and are selling them back to us…. as consumers.

CORPORATE AWARENESS OF DETAILS

Boards of Directors and investment leaders must begin to look beyond the next fiscal quarterly earnings call and begin to think strategically with respect to how their decisions and unawareness of the long-term threat impact their businesses and industries, which is woven with our national security, economic stability, and endurance of our republic.

In 2017, the Communist Party of China issued new state laws to facilitate the perniciousness of their efforts to obtain data, from everywhere. Three specific portions of those laws should be understood, and be an enduring reminder to CEOs, General Counsels, Chief Data Officers, CIOs, and CISOs, throughout our private sector ecosystems.

The first is Article 7 of the People's Republic of China National Intelligence Law summarily stating that all business and citizens *shall* cooperate with China's intelligence services and shall protect all national work secrets.

The second is Article 77 of the same National Security Law summarily stating that Chinese citizens and business *shall* provide anything required or requested by the Chinese government or intelligence services.

The third is Article 28 of the 2016 Cybersecurity Law summarily stating that all network operators *must* provide data to, and anything requested by, national, military or public security authorities.

Hence, if you are a U.S. business seeking to enter a business relationship with a company in, or from, China, your data will be obtained and provided to the MSS or PLA for their usage. This includes third party data as well. The analogy is a U.S. company enters into a business deal or partnership with a company from another country. The U.S. company must provide all relevant and requested data from their company, as well as the partner company, to the NSA, CIA and FBI.

CHINA DOES NOT PLAY BY ANY RULES

China plays by their own rules. China does not conform to any normalized set of regulations, guidelines, norms, laws or value-based agreements throughout the global economic ecosystem.

To further the CCP's unleveled economic playing field, out of the 15 largest companies inside China, 13 are either owned by the CCP, or run by the CCP. The world has seen recently what the CCP is capable of when one of the largest companies in the world, Alibaba, pushes back on state-run efforts. Additionally, many of the CCP's largest corporate leaders and CEO's have gone missing.

American business leaders, and Americans in general, must understand that China is a Communist Country run by an authoritarian "President" for life. Unlike in the U.S. and Western democracies, and like Putin's Russia, there is no bifurcation between the government, industry, and or criminal organizations.

ANALOGY

Hence, for a prospective business deal with a company in the U.S., the Chinese company can partner with China's intelligence services to assist in negotiations, vulnerabilities, and utilization of any already acquired data from said U.S. company. Again, this is akin to a U.S. based company calling he CIA and NSA for assistance on preparing a bid to merge with a company outside the U.S. and use all types of classified collection to form a proposal or use during negotiations.

DATA ACCUMULATION

The willingness of China, and its intelligence services, to illegally, and legally, obtain DATA to drive artificial intelligence, research and development programs, and to facilitate their military and economic goals without doing the hard work to independently develop on their own, drives at the heart of China's unfair practices. It is estimated that 80% of American adults have had all of their personal data stolen by the CCP, and the other 20 percent most of their personal data.

From genomics and DNA to third party financial data stored in cloud services providers, to fertility to Internet of Things technology, the effort du jour is accumulation of data, and lots of it.

SOCIAL CREDIT SCORE

China continues to surprise the world by aggressively stifling their citizens via laws, regulations, unparalleled domestic surveillance, and a debilitating Social Credit Score for every citizen. And a conversation about what is occurring the Uyghurs is for another hearing. It is important to remember that Chinese nationals, here in the U.S. are continuously monitored and their actions impact their credit score.

UNITED FRONT WORK DEPARTMENT

China's efforts to prohibit and violate free speech inside the U.S. must be identified, exposed and mitigated. China conducts such activities on Chinese nationals and on American citizens. Similarly, the CCP utilizes a suite of capabilities to silence critics here in the U.S. when the activity is exposed. The utilization of the United Front Work Department to drive false narratives in social media and within mainstream print and television media is consistent and enduring. There are numerous examples of such, however I want to reference just a few recent examples. The first is the Chinese Embassy in Washington DC pressuring Nobel scientists to censor their speeches at the 2021 Noble Prize Summit. The prize winners were bullied by the Government of China to disinvite the Dalai Lama for the award ceremony. The second example is Zoom executive charged for working with the Chinese intelligence services to disrupt Zoom calls in the U.S. commemorating Tiananmen Square. The third example is American actor John Cena apologizing, in Mandarin, because of the pressure Chinese officials placed on him, and Hollywood, because he referenced Taiwan as a country. The

pressure being placed by China on Hollywood has grown to a credibility questioning level and impacts just about every decision they make with respect to scripts and potential villains. This is referred to as "apology diplomacy" and has been publicly visible for many years when CEOs and company executives must apologize to Xi or the China for indiscretions with respect to referring to Taiwan as an independent country.

A final example, and one that really illustrates the granularity and scope of the CCP and UFWP, is when the CCP forced a small Jesuit high school in Colorado to change language on their web site to designate Taiwan as part of China. The CCP identified this when the high school applied for credentials to take part in the United Nations Commission on the Status of Women.

OPERATION FOX HUNT

One of the most disturbing, and illegal, activities by the CCP on American soils is Operation Fox Hunt. Operation Fox Hunt is an international effort by the CCP to identify, locate and attempt to bring back Chinese dissidents who have left China and are causing President XI and the Communist Party discontent. For almost a decade Chinese intelligence service have been building teams to conduct surveillance in the U.S., oftentimes falsely entering relationships with local law enforcement to garner information on who China claims are fugitives and attempt to bring them back to China. In January 2023, the FBI conducted a search warrant of a suspected Chinese police station in New York City which was furthering this effort, and most likely more undisclosed illegal activity.

The willingness, ability, and success of the Communist Party of China to conduct such aggressive activity within the confines of America's boarders is disturbing and unacceptable.

CYBER CAPABILITIES

From a cyber perspective, China has significant and unending resources to penetrate systems and obtain data, or sit dormant and wait, or to plant malware for future hostilities.

The FBI recently unveiled details for the first time on a 2011-2013 Chinese state-sponsored cyber campaign against U.S. oil and natural gas pipeline companies that was designed to hold U.S. pipeline infrastructure at risk.

Additionally, in July 2021, DOJ unsealed an indictment charging four individuals working with China's MSS for a global cyber intrusion campaign targeting intellectual property and confidential business information, including

infectious disease research. Targeted industries around the world included aviation, defense, education, government, health care, biopharmaceutical and maritime.

And lastly, in July 2021, NSA, FBI, CISA publicly released more than 50 cyber tactics and tools used by Chinese state-sponsored hackers against the U.S. as well as mitigation steps for US companies.

Over the past decade we have seen CCP cyber and insider threat breaches and criminality to such a level I fear we are becoming numb when it is identified. One such event was the Equifax breach in May of 2017. As a former head of U.S. Counterintelligence, I consider this to be one of the CCP's greatest intelligence collection successes. More than 145 million Americans had all their financial data, nicely aggregated, to the CCP along with Equifax's business process and trade secrets on how they acquire and share such data. That is every American adult.

Anthem lost 80 million medical records in 2015, Marriott lost 500 million guest's records in 2014, and in 2015 OPM lost 21 million records to China's cyber theft. I would be remiss if I left out China's breach of multiple cloud service providers in which China obtained access to over 150 companies' data.

INSIDER THREAT

The Insider Threat epidemic originating from the CCP has been nothing short of devastating to the U.S. corporate world. Anyone can go to Department of Justice's web site and search economic espionage. The result is hard to swallow and quantify. And those listed cases are just what was identified, reported by a U.S. company, and then prosecuted. I will touch on the impact of economic espionage a bit later.

In April 2021, a former scientist at Coca-Cola and Eastman Chemical was convicted of economic espionage & theft of trade secrets, on behalf of the CCP. The scientist stole trade secrets related to formulations for bisphenol-A-free (BPA-free) coatings for the inside of beverage cans. The scientist was working with a corporate partner inside China to monetize the stolen data utilizing the new company in China. The CCP had invested millions in the shadow new company in China. The stolen trade secrets cost US companies approximately $120 million to develop per open-source reporting. This is one example from the dozens identified in the past five years.

AGGREGATED CAPABILITIES

When you combine the persistence of intent and capability for the CCP's cyber intrusion programs, with the onslaught of Insiders being arrested, indicted and convicted by the FBI and DOJ over the past decade, it creates a formidable

mosaic of insurmountable levels. But it is not. With a comprehensive whole of government, and whole of society, approach of defending against China with awareness, strategy, enhanced defenses, practical mitigation programs, and a patriotic value-based return to great competition, the U.S. can begin change the course of history as I see it now.

SUPPLY CHAIN

So, what is current and next in the targeted view scope by the CCP? Look no further than President Biden's economic growth agenda and proposed congressional legislation detailing our strategic movement in the next few years. Electric vehicles, battery technology, bio agriculture, precision medicine and sustainable green energy. All of this is prime targets for penetration, and theft, buy the CCP. And at the same time, Ford Motor Company decided to partner with Contemporary Amperex Technology Co. Limited (CATL). This partnership is selfish, creates disincentive for investors to develop battery plans here in the U.S. Additionally, and more importantly, this partnership creates a critical supply chain dependency not only to the state sponsored CATL, but as well the CCP as a whole.

As an analogy, China manufactures, produces, and delivers 80 percent to the anti-biotics sold and utilized in the U.S. We cannot afford to continue to allow China to control and/or manipulate our critical and emerging supply chains and potentially hold us hostage in the future.

LEGITIMATE BUSINESS USED AS INTELLIGENCE GATHERING

China's strategic ability to utilize legitimate business ventures and investment in the U.S. that can also serve as intelligence collection and monitoring vehicles is comprehensive. It also provides the signature mosaic of how the best capitalistic economy the world has ever seen can be vulnerable to adversaries who hide their capabilities on our soil and in plain sight. Three simple and current event examples I will proffer is Huawei Technologies, farmland purchases near military installations, and ZPMC Cranes at critical U.S. maritime and military shipping ports.

MALIGN INFLUENCE

I would be remiss if I did not reference the strategic and aggressive nature in which the CCP conducts malign foreign influence in the U.S. Unlike Russia's persistent attempts to undermine our democracy and sew discord, the CCP strategically, and with precision, conducts nefarious influence campaigns at the state and local level.

I have referenced the influence success in Hollywood and the self-censoring which occurs to not offend China to ensure sales of their product to the Chinese markets. When it comes to Taiwan, the CCP becomes the most aggressive. Oftentimes state and local officials agree to travel to Taiwan to identify or negotiate economic investment opportunities. The CCP will undoubtedly apply holistic pressure to the local officials, from overt threats to subtle promises of economic infusion at the city or town level. There is most likely a company or business located inside an official's town which is heavily influenced or leveraged by prior investment by the CCP. China will apply pressure to that U.S. company and threaten to slow down production or manufacturing in China if the company officials do not apply their respective influence on the elected leader to not travel to Taiwan. This state or local official, or even U.S. Congressperson, may have no knowledge of China's intent beneath the surface. At the same time, and not coincidently, an op-ed or article will appear in the local newspaper downplaying economic investment opportunities in Taiwan and championing alternative efforts in China.

WHY IT ALL MATTERS:

In 2020, the estimated economic loss from the theft of intellectual property and trade secrets, JUST from the CCP, and JUST from known and identified efforts, is estimated between $300 Billion and $600 Billion per year (Office of the U.S. Trade Representative). To make it more relevant to Americans reading this, it is approximately $4,000 to $6,000 per American family of four…after taxes.

Additionally, in 2010 China had one company in the top ten of Forbes' Global 2000 list. In 2020 they had five. That is a 500 percent increase in one decade. Competition is great and necessary and is what made America the global leader we are today. However, I would proffer China's growth through any and all means is much less than fair competition. To reiterate, competition is always good, and necessary in any aspect. My question is…are we really competing? If we do not alter how we compete on the global ecosystem with awareness of China's methodology and practices, we will not be able to sustain or global position as the world leaders in technology, manufacturing, education, science,

medicine, research, development, and thoughts and ideas. We must aggressively enhance our willingness to not only understand these threats and unfair practices but be willing to create a robust public private partnership with intelligence sharing to combat the CCP while at the same time staying true to the values, morals, and rule of laws made America the greatest country in the world. Additionally, we must urgently decide that breaking the stranglehold of the CCP on our vast supply chain must end. The U.S. must engage in an aggressive and urgent redundancy effort and begin to have alternate servicing of goods, products and technologies.

PROTECT WHAT IS DEVELOPED

Congress's recent passage of a bill to bolster competition and provide the much-needed resources to do so is a great start down this long road. However, we must also protect the fruits of this legislative labor from being stolen and siphoned out of the U.S. by the same techniques China successfully utilizes today. Otherwise, we will continue to conduct research and development which the CCP will obtain, legally, and illegally, to bolster their economic, geopolitical and military goals of global dominance well into the future.

CLOSING

In closing, I would like to thank this Subcommittee, and the House Homeland Committee writ large, for acknowledging the significant threat posed by China, not only by holding this hearing, but with all the recent legislative actions the past year on combatting this threat as well as driving enhanced competition. Continuing to combat the threat posed by the CCP will take a whole of nation approach with a mutual fund analogous long-term commitment. Such an approach must start with robust and contextual awareness campaigns. The WHY matters. Regarding these awareness campaigns, we must be specific and reach a broad audience, from every level of government to university campuses, from board rooms to business schools, educating on how China's actions impair our competitive spirit by obtaining our research and development, trade secrets and intellectual property, and degrading our ability to maintain our role as economic global leaders. I have provided some recommendations for this committee, the IC, the administration, academia, research and development, as well as CEOs and board of directors in our holistic efforts to detect and deter these threats, as well as educate, inform, and compete.

Our nation needs strategic leadership now more than ever, particularly when we face such an existential threat from a capable competitor who is looking beyond competition to the global dominance.

Lastly, I would like to state for the record the significant national security threat we face from the Communist Party of China is NOT a threat posed by Chinese people, as individuals. Chinese Nationals, or any person of Chinese ethnicity here in the U.S., or around the world, are not a threat and should NOT be racially targeted in any manner whatsoever. This is an issue pertaining to a communist country, with an autocratic dictator who is committed to human rights violations and stopping at nothing to achieve his goals. As a nation, we must put the same effort into this threat as we did for the terrorism threat. The threat from China, particularly with respect to the long-term existential threat is hard to see and feel, but I would suggest it is much more dangerous to our viability as a nation.

Recommendations:

The holistic, and existential threat posed by the CCP is one of the few bipartisan agreements in the U.S. Congress today. We must take this opportunity to expeditiously advise, inform, and detail the threat to every fabric of our society, and why it matters. We must, as a nation, compete at the highest level possible while at the same time understand why we are doing so, and what is at stake.

1. Enhanced and aggressive real time and actionable threat sharing with private sector. Create an Economic Threat Intelligence entity which delivers actionable, real time threat information to CEOs, Boards of Directors, state and local economic councils to enable risk-based decision making on investments and partnerships. The analogy would be the Financial Services ISAC. This intelligence delivery mechanism should include the Intelligence Community, FBI, and CISA and have at is core constituency state and local entities at risk and utilize existing vehicles such National Governors Association and the Chamber of Commerce to increase threat awareness of illicit activities investment risk at the state and local level.

2. Congress must ensure U.S. government agencies are leaning aggressively forward in providing collected intelligence pertaining to plans and intentions, as well as nation state activities, in software, coding, supply chain and zero-day capabilities. The U.S. Government must be more effective in providing intelligence to the private sector. Enhanced declassification of collected intelligence with respect to threats to our economic well-being, industries, and companies must be delivered at speed to impacted entities prior to the threat becoming realized.

3. Bipartisan congressionally led "China Threat Road Shows" to advice and inform of the threat to CEOs, Governors, and Boards of Directors in critical economic, research and manufacturing sectors.

4. Close governance and oversight of China Competition legislation with measurable outcomes and effectiveness reviews. Particularly in the research and development space.

5. Create a panel of CEOs who can conversely advise and inform Congress, the IC, and U.S. Government entities on perspectives, challenges, and obstacles in the investment arena and private sector. Currently, there is no such venue existing. I would recommend a *Business Round Table* type of framework. Membership should be diverse and include but not limited to the following sectors: Financial Services, Telecommunications, Energy, Bio Pharmaceutical, Manufacturing, Aerospace, Transportation, Private Equity and Venture Capital. Select key government participants and encourage actionable outcomes. This entity should be co-chaired by a CEO form this group.

6. Create a domestic version of the State Department's Global Engagement Center. The U.S. government needs a "sales and marketing" capability which can partner with U.S. business and academia to guide new and emerging threat intelligence, answer pertinent questions, and construct awareness campaigns against the threat from the CCP and other similar issues.

7. Establish an over-the-horizon panel to discuss, in a public forum, emerging threats posed to the long-term economic well-being of America. The first topic should take a close look at the strategic investments the CCP is making into state and local pension plans, as well as the Federal Thrift Savings Plan.

8. Immediately create a Supply Chain Intelligence function which can sit both in the U.S Government, as well as outside of government, to facilitate real time intelligence sharing. This entity should include members of the private sector skilled in understanding our supply chain and who can expedite reacting to emerging threats. This entity will also be able to provide the U.S. Government cogent mitigation strategies and

assistance with policy formulation to protect our vulnerable supply chain from persistent penetration and manipulation by China and Russia.

9. STEM must become a U.S. educational priority once again. It must be funded, focused, measurable, and begin at the earliest stages of the K through 12 educational tracks. It must also be looked upon as a long-term project (25 years).